BY ORDER OF THE COMMANDER ***LAUGHLIN AFB INSTRUCTION 10-2***

14 August 1997

Operations

OPERATIONS SECURITY (OPSEC) INSTRUCTIONS

Purpose Statement: The instruction implements and executes the general guidance of AFI 10-1101, *Operations Security (OPSEC) Instructions*, for the 47 FTW. It does so with regard and sensitivity to the particular manning, assets, mission, location and overall situation of Laughlin AFB and of the 47 FTW.

1. The Concept of Operations Security within the 47 FTW:

1.1 Prudent OPSEC discipline and practice is required as the 47 FTW is replete with critical information. With the 47 FTW Joint Specialized Undergraduate Pilot Training program, these include indicators of both the manning strength and general competence level of the Air Force's future pilot corps--a significant piece to the puzzle!

1.2 Examples of other OPSEC critical information and measures are outlined in attachment 1 of this supplement. This list is intended to draw attention to some of the more common indicators and is not all-inclusive.

1.3 A particular concern at Laughlin AFB is its proximity to the Mexican border. This allows adversaries collecting against the 47 FTW to operate from the sanctuary of foreign soil and an opportunity to quickly and easily flee from U.S. authorities. Most nations have embassies in Mexico City which is historically a route to pass sensitive or even classified information to our adversaries. In addition, there is a potential heightened threat to the base from drug trafficking, illegal immigrants, and suspected terrorist groups. All 47 FTW personnel should be aware of these special threats to Laughlin AFB.

2. 47 FTW Operations Security Process:

2.1 The 47 FTW OPSEC Manager ensures each unit OPSEC monitor is thoroughly familiar with the Operations Security Process, as described in AFI 10-1101, *Operations Security (OPSEC) Instructions*, Chapter 2.

2.2 Individual unit OPSEC monitors ensure personnel within their units, especially those who handle or have access to material or information which may be sensitive or exploitable, are familiar with the basics of the Operations Security Process.

2.3 The 47 FTW OPSEC Manager supports the unit programs through information, consultation, and materials to the fullest extent possible.

3. 47 FTW Operations Security Program:

3.1 The 47 FTW OPSEC program is an integral part of the overall Air Force program. OPSEC is a process of identifying indicators and analyzing friendly actions to reduce vulnerabilities and deny critical information to our adversaries.

Supersedes 47 FTW Instruction 10-2, 5 October 1995
OPR: 47 OSS/OSIN (Capt Kelly K. Fedel)
Certified by: Lt Col Brian C. King
Printed Pages: 4/Distribution:F;X:
HQ AETC/CEMG-1

3.2 The 47 FTW OPSEC Manager, unit OPSEC monitors, commanders and first sergeants must all be familiar with the Air Force OPSEC Program as described in AFI 10-1101, Chapter 3. In addition, other personnel, particularly those directly involved with sensitive or exploitable material or information, must be familiar with this program.

3.3 An OPSEC Working Group will meet at least annually to discuss the 47 FTW OPSEC Program. This board may be convened by the 47 FTW Commander or the FTW OPSEC Manager at any time.

3.4 The OPSEC Working Group will consist of the primary and alternate 47 FTW OPSEC Managers and unit OPSEC monitors and/or designated alternates. The 47 FTW Security Manager and OSI representative can also be invited to observe and consult during the meetings, although this is not mandatory.

4. Operations Security Programs Subordinate to the 47 FTW:

4.1 All squadron commanders will appoint a primary and alternate officer or NCO to be the organizational OPSEC monitor. The alternate need not to be of lower rank than the primary.

4.2 Group commanders are not required to appoint group OPSEC monitors, but may do so at their discretion. Group and wing administrative sections may be incorporated into a related unit OPSEC program.

4.3 Appointment letters naming each unit's OPSEC monitors will be accomplished and forwarded to the 47 FTW OPSEC Manager.

4.4 Unit OPSEC managers will maintain a unit OPSEC continuity binder with the following at a minimum:

4.4.1 Appointment letter(s)
4.4.2 AFI 10-1101
4.4.3 AETC Supplement 1 to AFI 10-1101
4.4.4 47 FTW Instruction 10-2 (this document)
4.4.5 Current copy of unit OPSEC critical information
4.4.6 List of OPSEC training sessions, attendance, and topics
4.4.7 OPSEC self-assessment and/or compliance guides
4.4.8 Tasking and informational letters from 47 FTW OPSEC Manager

4.5 Unit OPSEC monitors will submit a unit OPSEC status report to the 47 FTW OPSEC Manager by 1 Jun of each year.

5. OPSEC Critical Information:

5.1 OPSEC Critical Information (CI) must be protected from loss to keep our adversary from gaining a significant operational, economic, political, or technological advantage, and to prevent adverse impact on friendly mission accomplishment.

5.2 Each unit OPSEC monitor will determine unit specific CI and provide a list in a format similar to attachment 1 of this instruction. A copy must be forwarded to the 47 FTW OPSEC Manger.

5.3 Unit OPSEC monitors will review and update their organization's OPSEC indicators annually. Current listings will be forwarded to the 47 FTW OPSEC Manager by 1 Jun each year. If there are no changes to the unit's listing from the previous year, an official letter stating the unit's OPSEC CI list was reviewed and no changes are required is adequate. Supplementary listing updates may be submitted by any unit OPSEC monitor to the 47 FTW OPSEC Manager at any time.

6. OPSEC Protective Measures:

6.1 The responsibility to protect OPSEC Critical Information rests with each individual assigned to 47 FTW. All actions, activities, and processes must be examined to determine whether information is adequately protected and if not, procedures must be changed to protect these indicators.

6.2 OPSEC protective measures can be an action, device, procedure, or technique to effectively reduce anyone's ability to exploit vulnerabilities. Possible protective measures include:

6.2.1 Mark appropriate documents "For Official Use Only"
6.2.2 Protect information as "need to know"
6.2.3 Password protect electronic information
6.2.4 Control entry with proper credentials or badges
6.2.5 Properly handle Privacy Act information
6.2.6 Authorize release of information by Public Affairs only
6.2.7 Minimize copies produced
6.2.8 Limit distribution lists
6.2.9 Properly mark and control classified

7. OPSEC Training:

7.1 The 47 FTW OPSEC Manager is responsible for training unit OPSEC monitors. Unit OPSEC monitors are responsible for all OPSEC training within their units.

7.2 According to AFI 10-1101 (para 4.8), OPSEC training must be mission-related, tailored to an individual's duties and responsibilities, and continue throughout each airman's career. To meet these requirements, unit OPSEC monitors will develop a unit specific OPSEC training program. The 47 FTW OPSEC Manager will consult and assist in developing and implementing these unit training programs.

7.3 At a minimum, unit OPSEC monitors will ensure newly assigned personnel, military and civilian, receive initial OPSEC training within 90 days of their arrival and that this training is documented. Additionally, unit OPSEC monitors will provide annual refresher training. Units with access to sensitive or exploitable material or information should determine if, and how frequently, specialized OPSEC training is accomplished within their unit to familiarize their personnel with job-related OPSEC considerations.

GARY A. WINTERBERGER, Colonel, USAF
Commander

OPSEC CRITICAL INFORMATION
Example Squadron
(date)

ACTIVITY	CRITICAL INFORMATION
Daily Operations	Accountability records
	Administrative organization
	Position descriptions
	Mission statements
	Distinguished visitors
	Checklist procedures
	Computer requirements
	Mission designators
	Inspection results
	International agreements
	Limiting factors
	Proficiency reports
General Deviations	Augmentees
	Backup resources
	Critical timing
	Deficiencies
	Efficiency measures
	Emergency procedures
	Exercise rehearsals
	Schedule modifications
	Accident/mishap reports
	Security investigations
	Personnel shortages
Personal Affairs	Access lists
	Readiness ratings
	Immunization records
	Security clearance
	Powers of Attorney & Wills
	TDY Orders
	Specialist requirements
	Unfavorable information
Communications	Assigned frequencies
	Message delivery efficiency
	Net/circuit designators
	Nodes and choke points
	Communications degrades
Electronic Activity	Navaids/TACAN beacons
	Radar coverage
	Radar procedures
	Search and rescue beacon

ACTIVITY	CRITICAL INFORMATION
Engineering & Services	Billeting capacity
	Engineering studies
	Environmental impact
	Structural capabilities
	Damage assessments
Financial Activity	Budget analysis
	Justification & Summaries
	Projections & Estimates
	Operating budgets
	TDY fund limits
Logistic Support	Shipment priority
	Courier service
	Nodes/choke points
	Control numbers
Maintenance	Downtime for repairs
	Equipment calibration
	Equipment nomenclature
	Maintenance trends
	Mission/sortie number
	Repair scheduling
	Failure rates
Operational Flying	Flight patterns
	FAA flight plan information
	Endurance capability
	Tactical formations
Planning	Command & Control
	Force composition
	Reaction times
	Threat assumptions
Public Relations	Contractor advertisements
	Legal publications
	Security & Warning notices
	Public appearances
Supply	Storage capacity
	Fuel loads/records
	Transfer rate/capacity
	Materials delivery
	Parts reliability
	Stockpile conditions
System Operations	Design factors
	Frequency range
	Product flow/volume
	Physical security systems